

IMSOLO-IV Forensics Quick Start Guide

(Rev. 2.3)

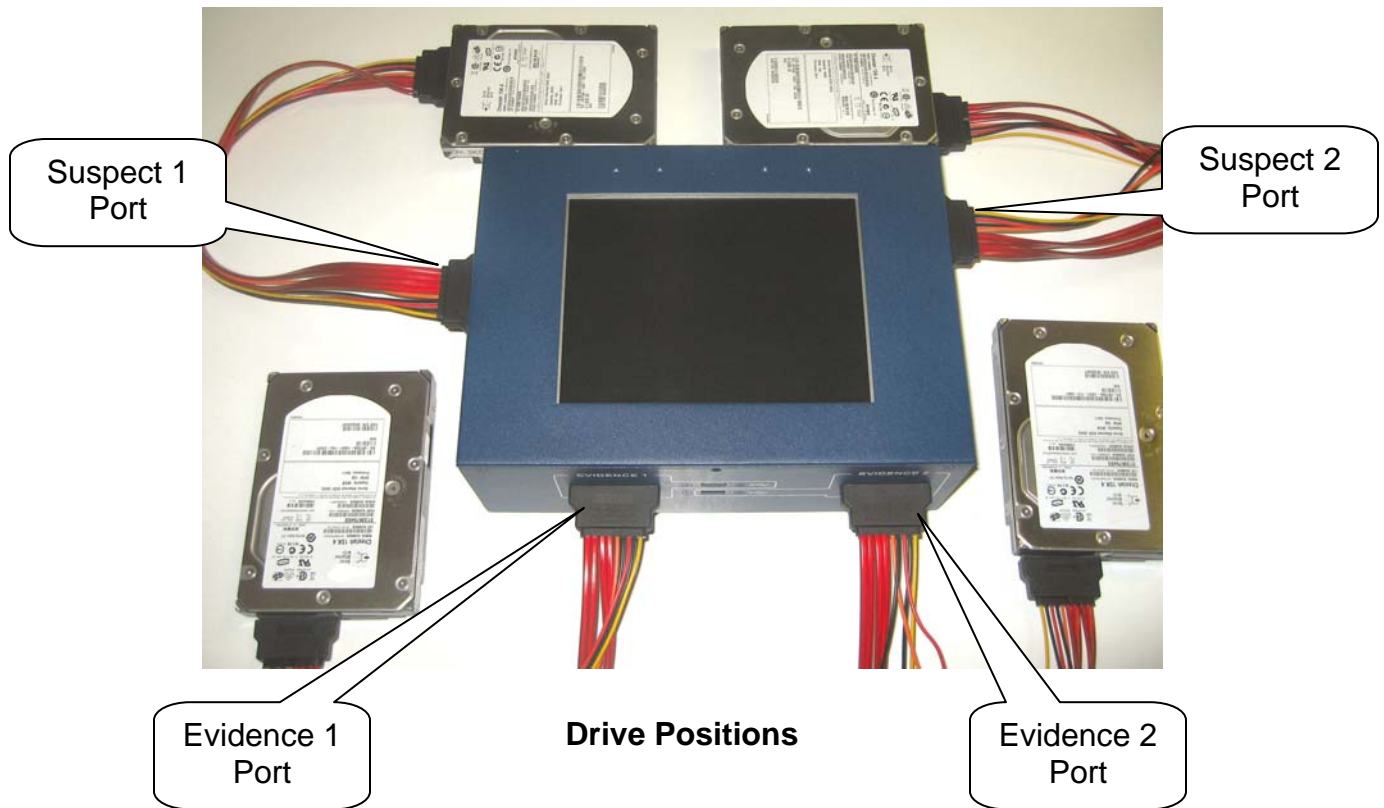
Please refer to the *IMSolo-IV Forensics User's Manual* for detailed instructions. The User's Manual is located on the supplied CD labeled "IMSolo-IV User's Manual". Also included is the *IMSolo-IV Expansion Option Quick Start Guide*. Updated User Manuals and Software are available at www.ics-iq.com or www.icsforensic.com.

1. Place the *IMSolo-IV Forensics* on a level surface.
2. Attach the AC power cord to the unit's power supply, located on the unit's back panel, and to an electrical outlet. The voltage may be either 110v or 220v. The unit will automatically switch to use either voltage.
3. Power ON the unit by pressing the unit's Power ON button, located on top corner of the unit's back panel. The *IMSolo-IV Forensics Advanced Interface Control Console* will be displayed.

The screenshot displays the 'Advanced Interface Control Console' software. The interface is divided into several sections. At the top, there are tabs for 'Main', 'Settings', 'Case Info', 'Detection', 'Mount Drive', 'HPA/DCO', 'Log', and 'Tools'. The 'Main' tab is active, showing a table for 'SUSPECT DRIVE' and 'EVIDENCE DRIVES' with columns for 'MB/min' and 'POSITION'. Below these tables is a section for 'OTHER DETECTED DRIVES'. The 'LinuxDD Settings' section includes a 'Capture File Size' dropdown set to '4.7GB (DVD)', a 'Custom File Size (MB)' input set to '4812', and a 'File name' text box. The 'Select Hashing methods' section shows 'Hardware accelerated' selected, with 'SHA1' and 'SHA2 (256)' checked. Other options include 'SHA2 (224)', 'SHA2 (384)', 'SHA2 (512)', 'CRC32', 'MD5', 'Encrypt/Decrypt', 'Read Back-Verify', and 'Hash Targets'. The 'Type of Operation' is set to 'LinuxDD Capture', with 'Start' and 'Abort' buttons. The bottom section shows 'Load Size (MB)' as 0, 'Time Left' as 00:00:00, 'Speed (MB/min)' as 0, 'Elapsed Time' as 00:00:00, and 'Copied (MB)' as 0 with a progress bar at 0%. At the very bottom, there are buttons for 'Advanced Screen', 'Operator Screen', 'Wizard Screen', 'On-Screen Keyboard', 'Next Copy Session', 'New Copy Session', 'Desktop', 'Exit', and 'About'.

Advanced Interface Control Console

4. Attach the ICS supplied SATA/SAS drive data/power cables to the unit's Suspect and Evidence connectors and to the SATA or SAS drives. For PATA drives use the supplied ICS SATA-to-PATA Adapter and connect the supplied PATA data cable's "Unit Side" connector to the Adapter's data connector and the "HDD Side" connector to the drive.



5. Select the Mode of Operation from the *Operations* pull down menu.

The screenshot shows the LinuxDD software interface with the **Settings** tab selected. The interface is divided into several sections:

- Top Tabs:** Main, Settings (selected), Case Info, Detection, Mount Drive, HPA/DCO, Log, Tools.
- Drive Selection:**
 - SUSPECT DRIVE:** Table with columns MB/min and POSITION.
 - EVIDENCE DRIVES:** Table with columns MB/min and POSITION.
 - OTHER DETECTED DRIVES:** Table with column POSITION.
- LinuxDD Settings:**
 - Capture File Size:** 4.7GB (DVD) (dropdown)
 - Custom File Size (MB):** 4812 (input)
 - File name:** (text input)
- Select Hashing methods:**
 - Hardware accelerated:** (checkbox)
 - SHA1:** (checkbox)
 - SHA2 (224):** (checkbox)
 - SHA2 (256):** (checked)
 - SHA2 (384):** (checkbox)
 - SHA2 (512):** (checkbox)
 - CRC32:** (checkbox)
 - MD5:** (checkbox)
- Operational Modes:**
 - Encrypt/Decrypt:** (checkbox)
 - Read Back-Verify:** (checkbox)
 - Hash Targets:** (checked)
- Type of Operation:** LinuxDD Capture (dropdown)
- Buttons:** Start, Abort
- Progress/Status:**
 - Load Size (MB):** 0
 - Time Left:** 00:00:00
 - Speed (MB/min):** 0
 - Elapsed Time:** 00:00:00
 - Copied (MB):** 0
 - Progress:** 0%
- Bottom Buttons:** Advanced Screen, Operator Screen, Wizard Screen, On-Screen Keyboard, Next Copy Session, New Copy Session, Desktop, Exit, About.

Callouts in the image:

- Drive Selection Panel:** Points to the 'Suspect 1', 'Suspect 2', 'Evidence 1', and 'Evidence 2' checkboxes.
- Operational Modes:** Points to the 'Hash Targets' checkbox.

6. Select the drives to be used for the selected operation from the *Drive Selection Panel*.
7. Verify all remaining applicable settings and optionally enter Case Information using the CASE INFO screen functions. It is recommended to enable the *Hash Targets* function. Selecting *Hash Targets* will result in the Capture operation generating the Hash value for the data read from the Suspect drive and the data written to the Evidence drive. After all the data is written to the Evidence drive, the Capture operation will generate the Hash value for the data read from the Evidence drive.



Hash values generated during the capture operation are generated for the data read from the Suspect's drive not from the data read from the Evidence (target) drive, unless the unit is instructed to hash the Evidence drive(s) by enabling the *Hash Targets* function. As an alternative, the Evidence Drives can also be hashed after the capture operation using the *Hash* mode of operation.

8. Select **START** to begin the operation. Operational status information will be displayed during an operation.
9. After the operation completes, the drives will be powered OFF and the drives can be safely removed. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails. Log files will automatically be stored internally and can be transferred to external media using the unit's USB ports, located on the back of the unit.

NOTE: The unit can be powered OFF by pressing and releasing the unit's Power button, located on the top corner of the unit's back panel.